ABSTRACT

The practical benefit of the inventive idea results from an assumption that typically, the operational subCAs will not get compromised. Assuming this, a a batch of revocation lists manifesting no revocations can be generated and signed. These pregenerated CRLs (root CRLs) can then be stored outside the high-security vault and, in case of no subCA compromises, published periodically one at a time to the directory system where the PKI clients can automatically fetch them.